

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І
АРХІТЕКТУРИ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ



ПРЕЗЕНТАЦІЯ

ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ МАГІСТРА

на тему: «Технологія інтелектуального захисту інформації
критично важливих об'єктів»



Виконав студент 2-го курсу, групи БІКСм-24
Андрєєв Марк Анатолійович.
Науковий керівник:
к.т.н., доцент Шабала Є.Є.

Актуальність проблеми: У зв'язку зі зростанням складності та різноманітності кіберзагроз, а також з урахуванням обмежень традиційних методів діагностики, актуалізується необхідність розробки ефективних підходів до захисту критично важливих об'єктів в умовах розподілених систем.

Метою дослідження є розробка технології інтелектуального захисту, що забезпечує комплексну діагностику, своєчасне виявлення аномалій та підвищення надійності критично важливих об'єктів на основі аналізу мережевого трафіку. Для досягнення поставленої мети визначено наступні завдання:

- Розробка підходу до комплексної діагностики.
- Виявлення мережевих аномалій для своєчасної ідентифікації загроз.
- Підвищення рівня надійності, стабільності та безпеки критичної інфраструктури.

Наукова новизна полягає в інтеграції концепцій та технологій, таких як штучний інтелект, машинне навчання та аналіз великих даних, в єдину систему інтелектуального захисту критично важливих об'єктів.

Предметом дослідження є методи та засоби діагностики мережевих аномалій на основі аналізу мережевого трафіку, застосовані для інтелектуального захисту критично важливих об'єктів.

Об'єктом дослідження є комп'ютерна мережа з багаторівневою системою безпеки, що імітує структуру критично важливого об'єкта і потребує ефективних методів захисту від кіберзагроз.

Задачі

1. Провести аналіз загроз кібербезпеці критичної інфраструктури та сучасних стандартів захисту критично важливих об'єктів (КВО).
2. Дослідити сучасні підходи до моніторингу та аналізу мережевого трафіку.
3. Розглянути методи виявлення та прогнозування мережевих аномалій.
4. Проаналізувати алгоритми машинного навчання та глибокого навчання, які можуть бути застосовані для інтелектуального захисту КВО.
5. Розробити структурну та функціональну моделі технології інтелектуального захисту інформації КВО.
6. Розробити та обґрунтувати архітектуру системи захисту КВО на основі машинного навчання та систем фізичного захисту

Класифікація об'єктів критичної інфраструктури



Потенційні впливи на об'єкти критичної інфраструктури

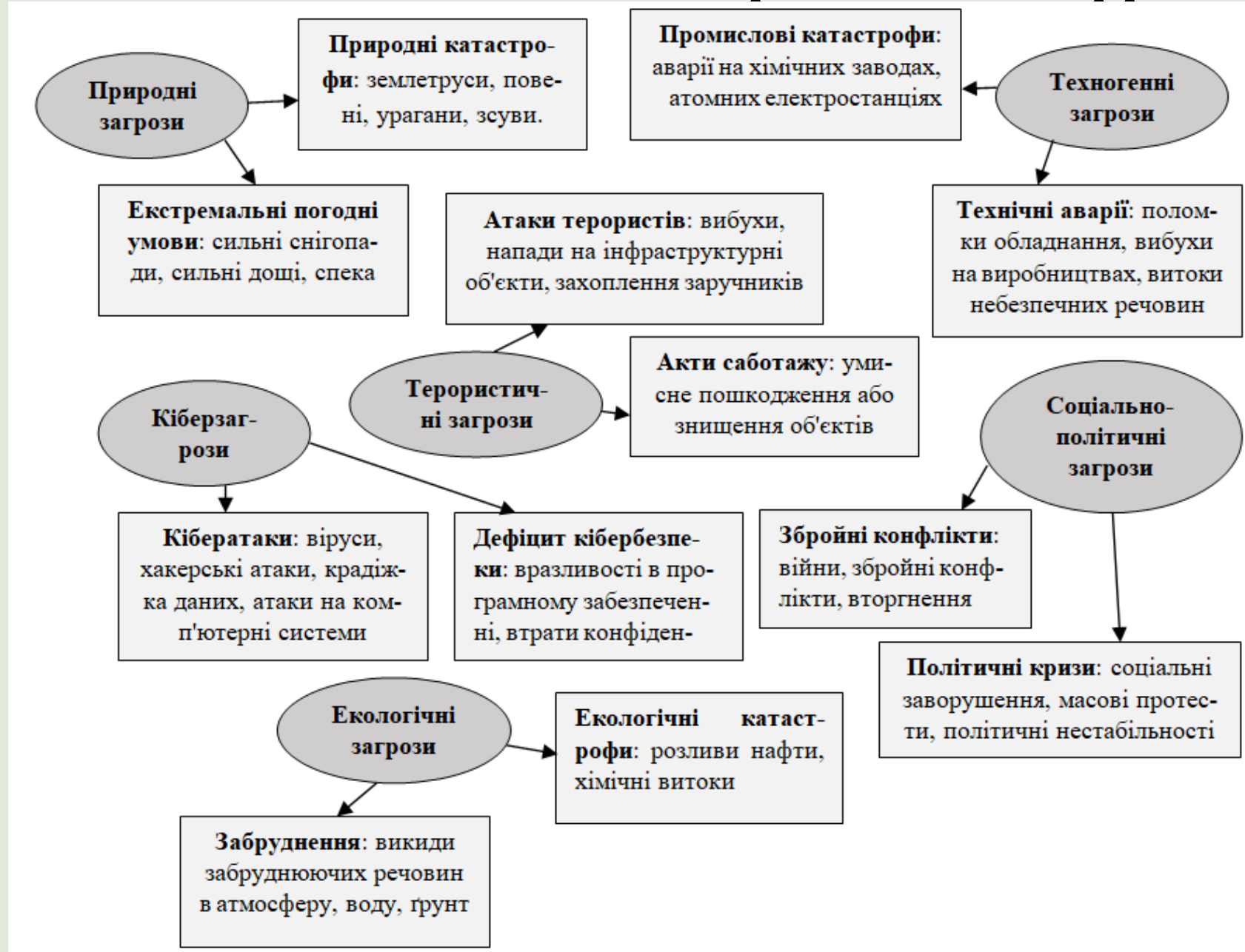
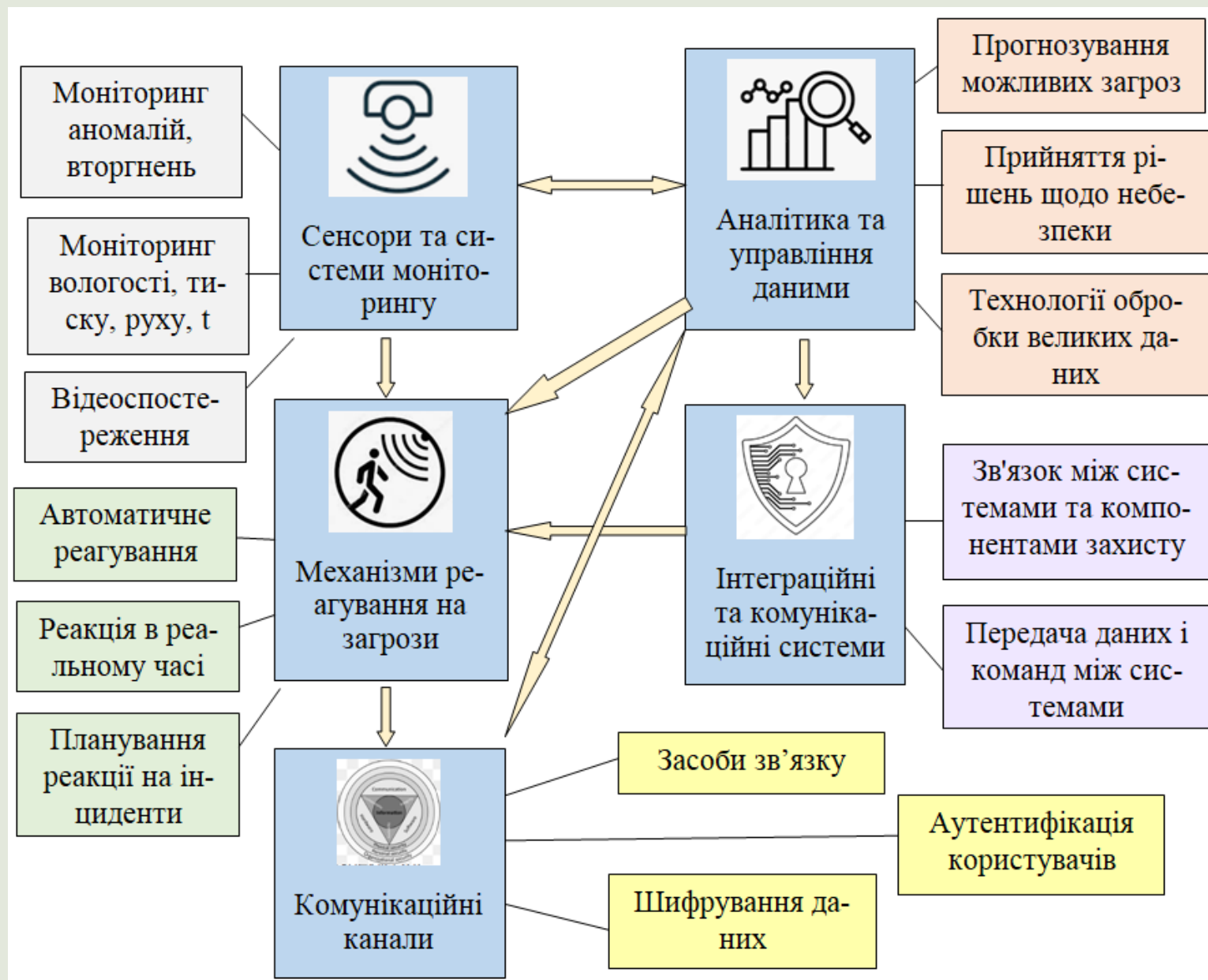
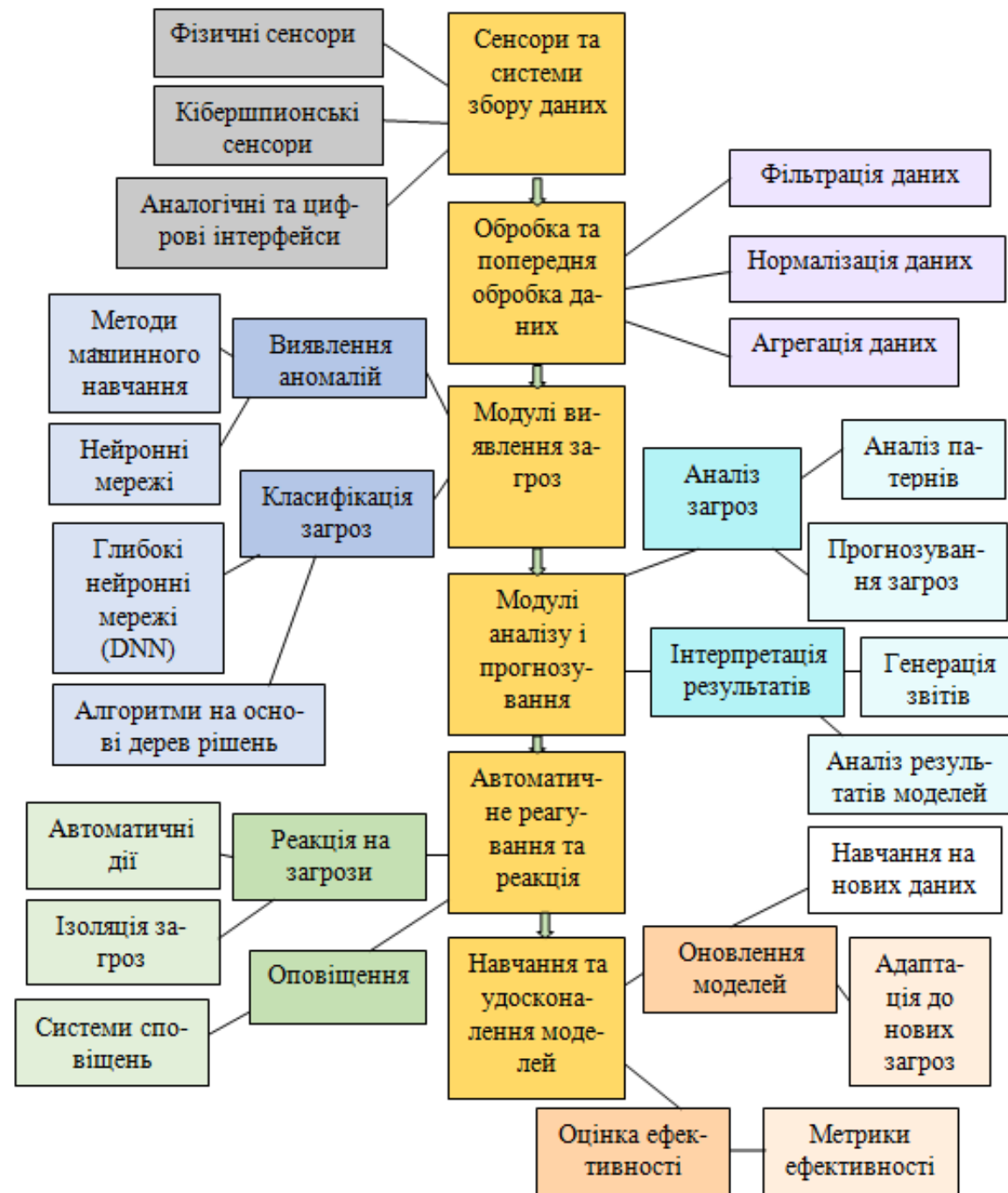


Схема архітектури системи інтелектуального захисту критично важливих об'єктів

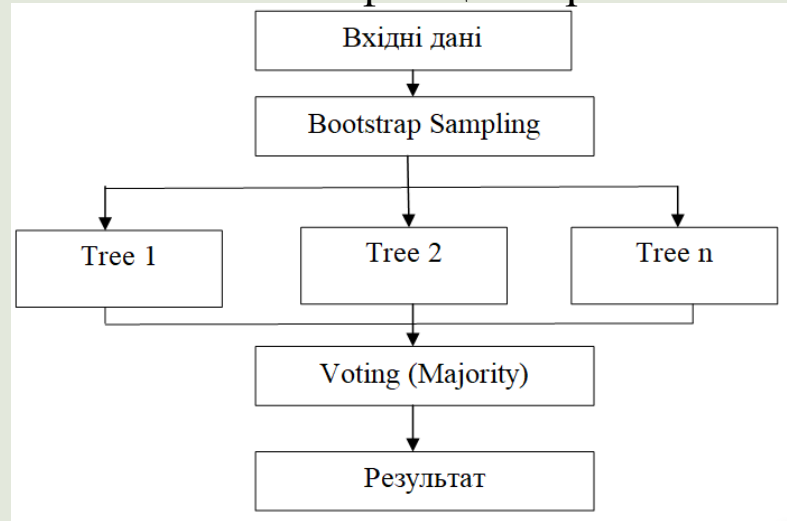


Архітектура системи штучного інтелекту для захисту критично важливих об'єктів



Модулі виявлення загроз

Схема алгоритму Random Forest для класифікації загроз



Алгоритм застосування K-means для захисту критичної інфраструктури

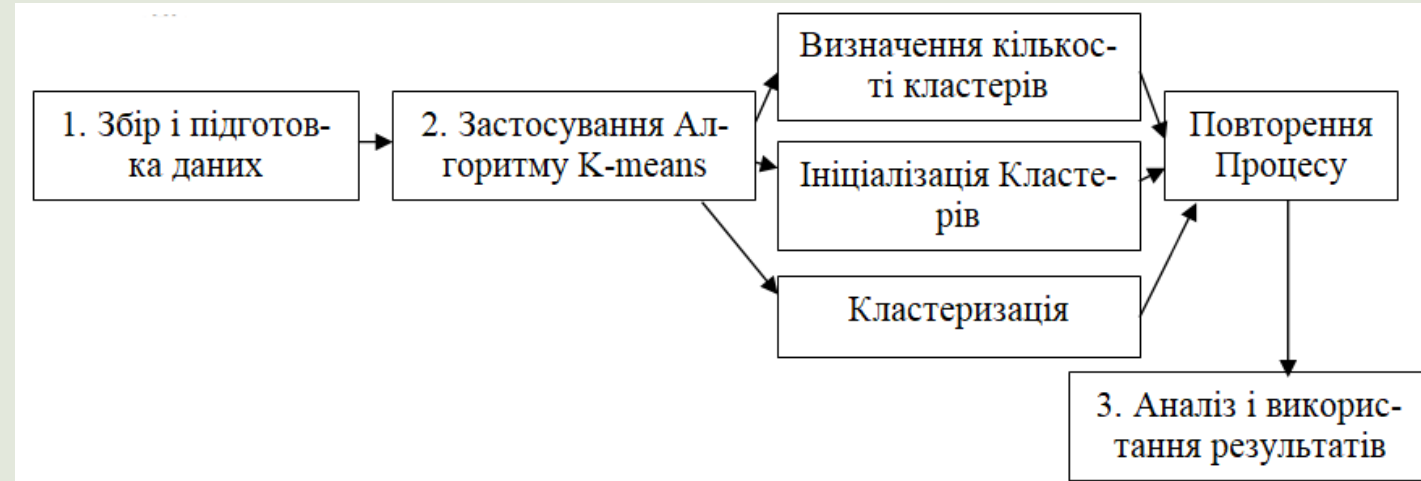
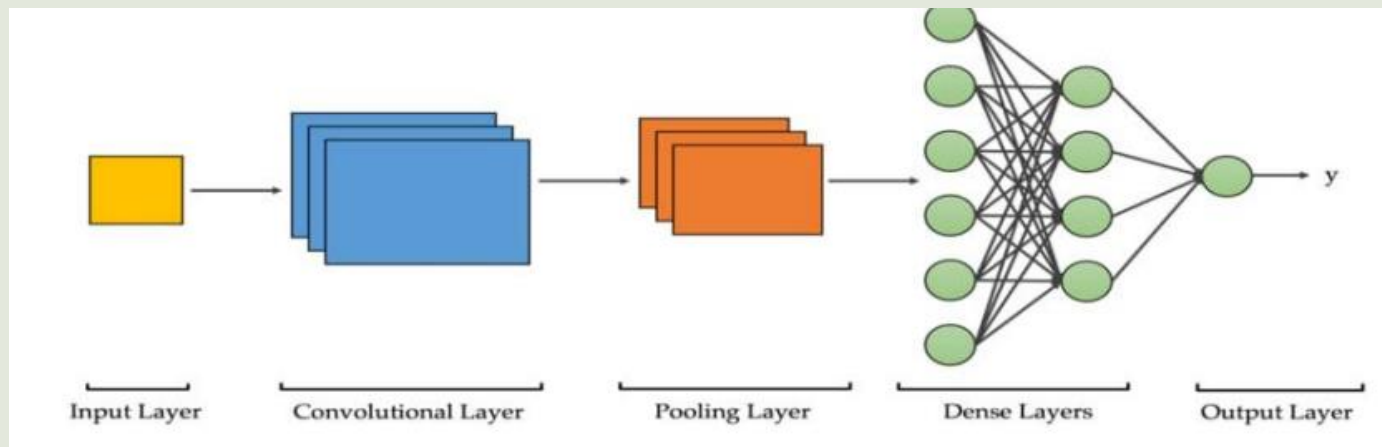


Схема архітектури згорткової мережі



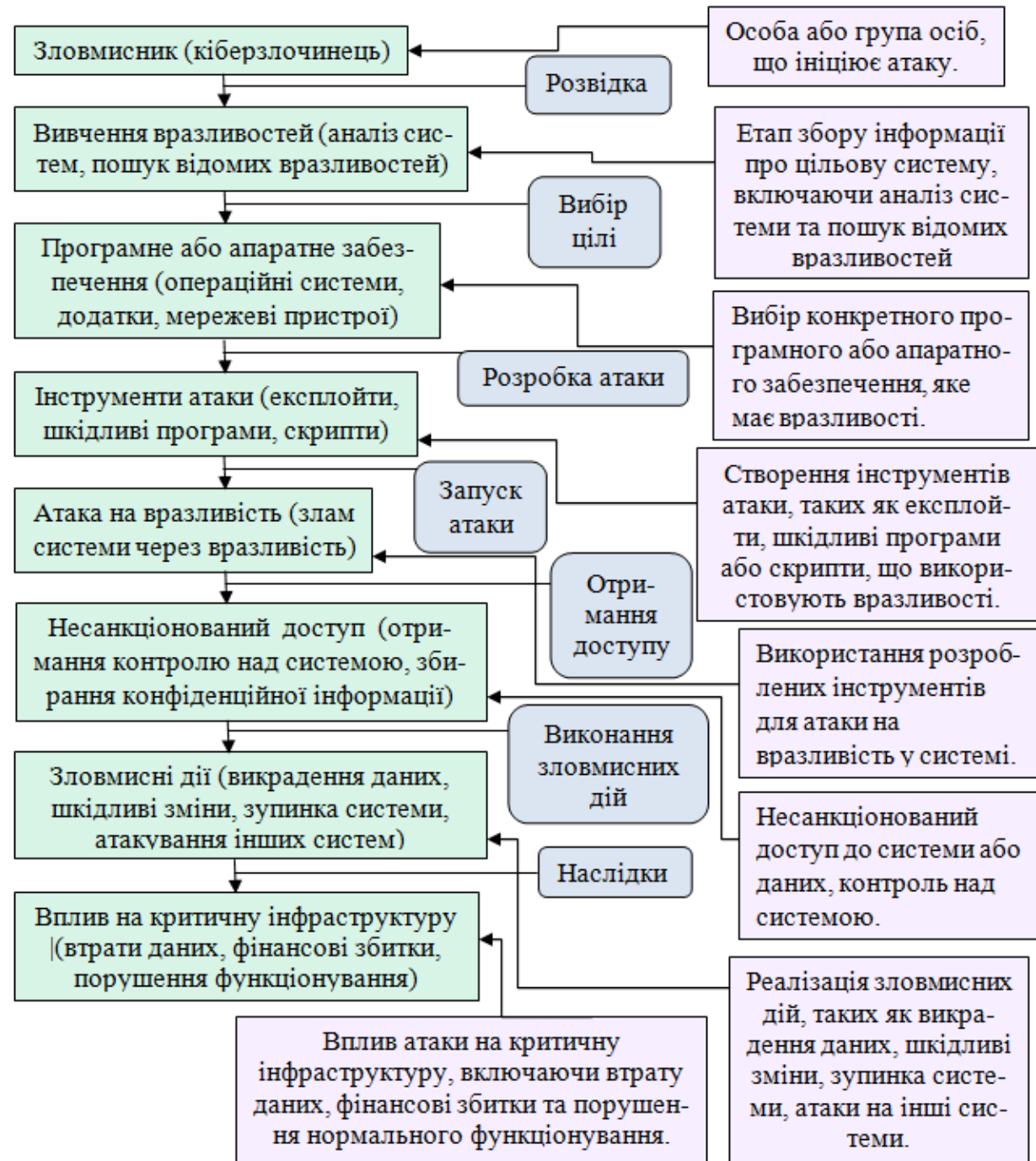
Застосування IoT в системах інтелектуального захисту критично важливих об'єктах



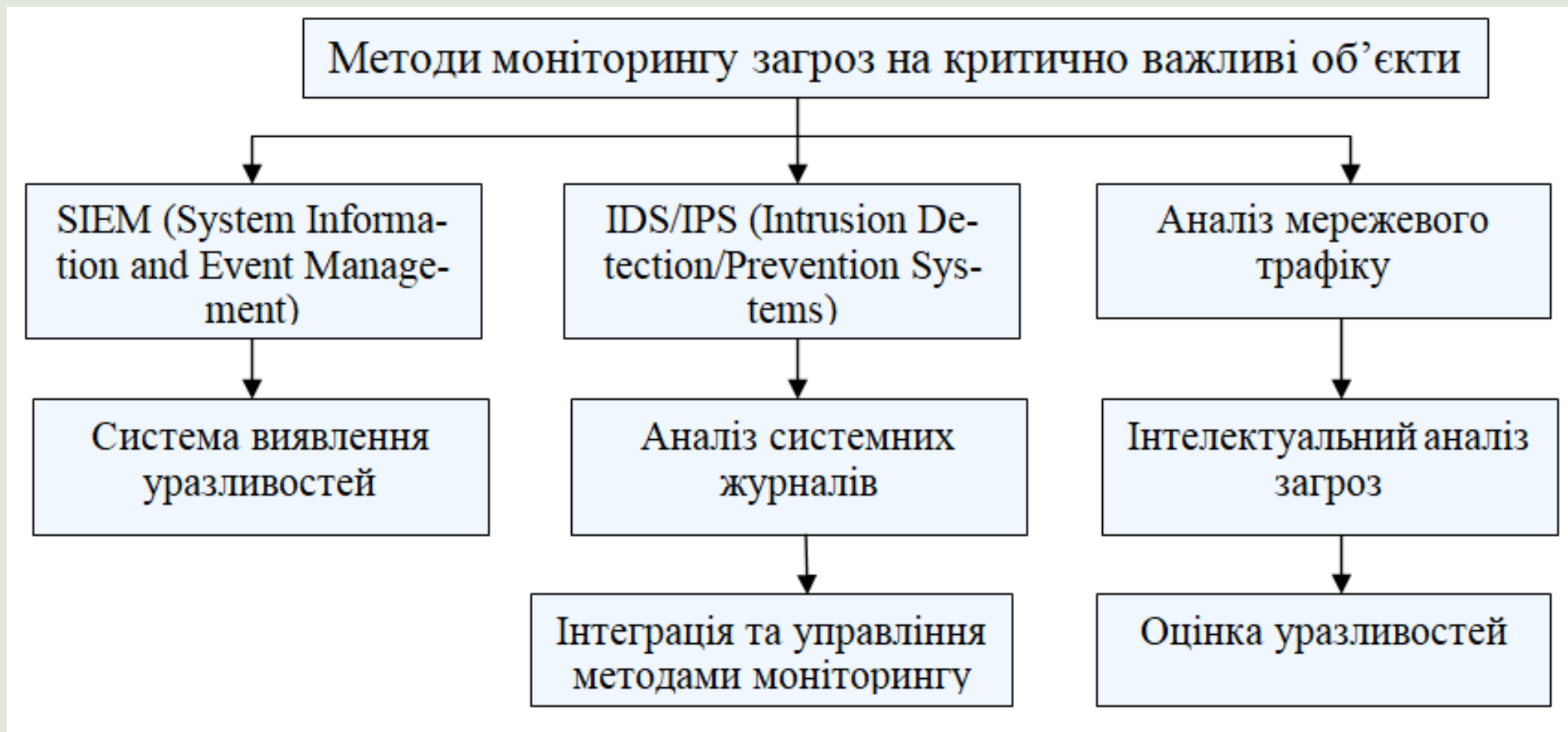
Модель DDoS атаки на критичну інфраструктуру



Модель атак, спрямовані на використання вразливостей програмного чи апаратного забезпечення на критичну інфраструктуру



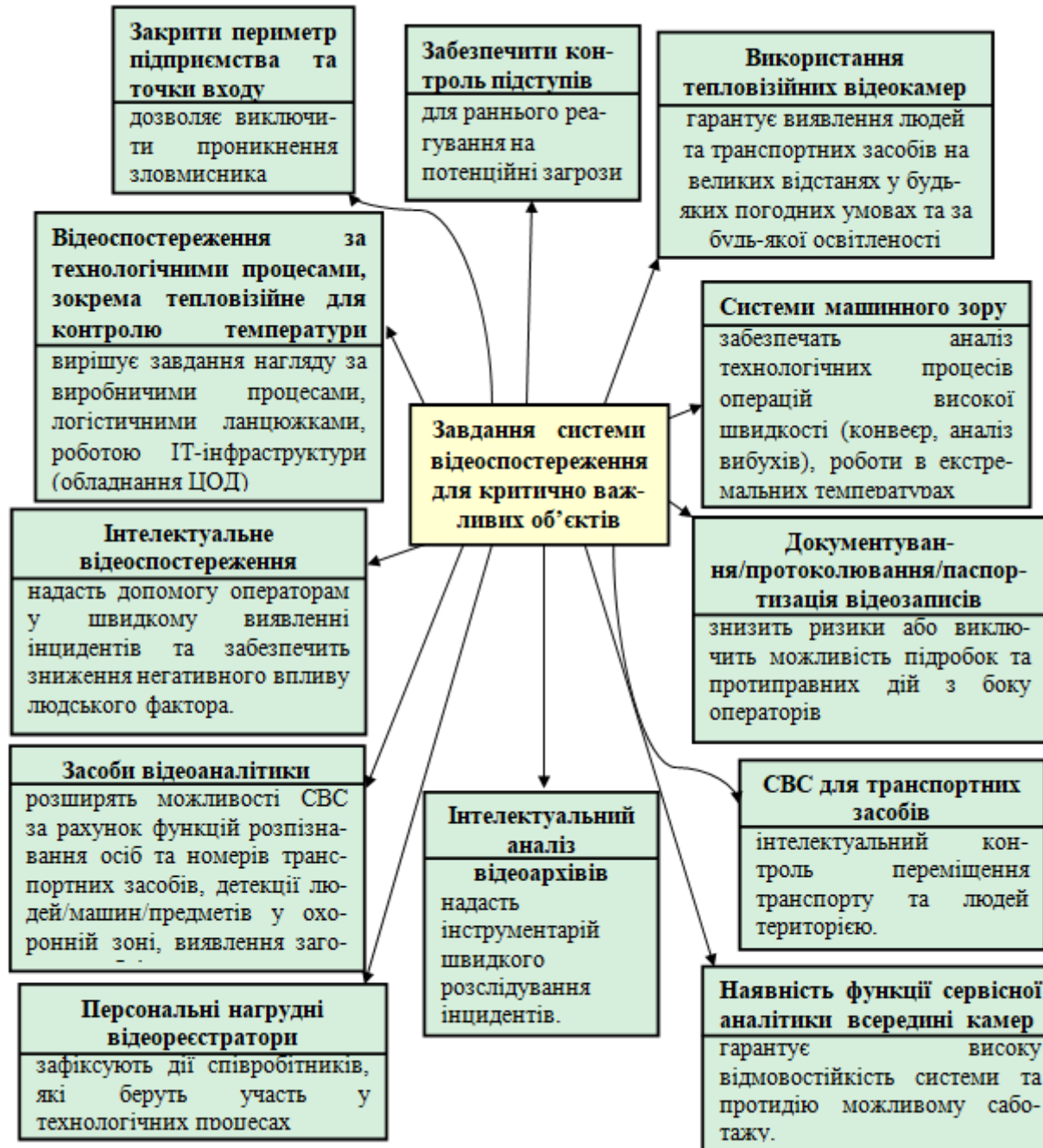
Методи моніторингу загроз на критично важливі об'єкти



Алгоритм реагування на інциденти загроз на критичну інфраструктуру



Завдання системи відеоспостереження для критично важливих об'єктів

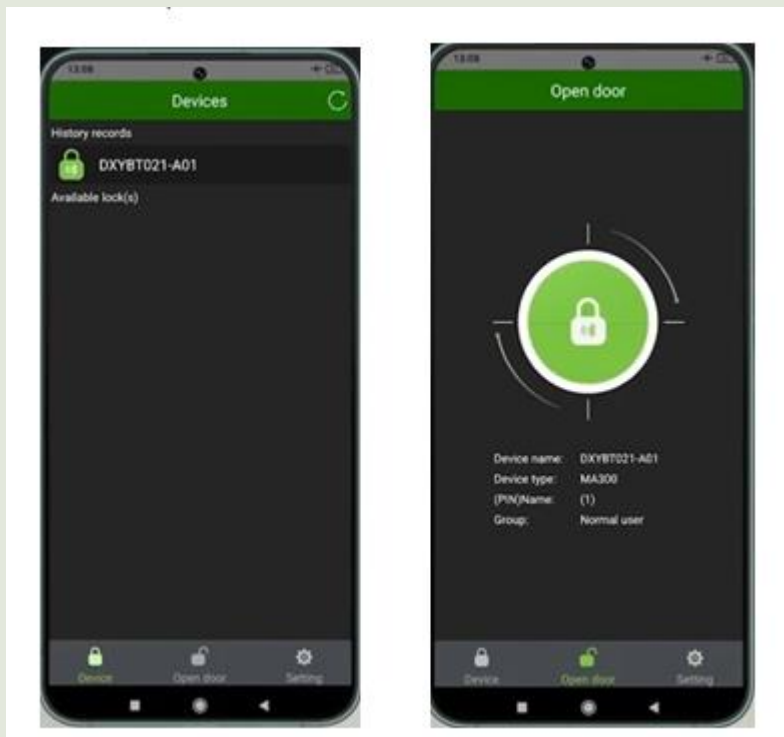




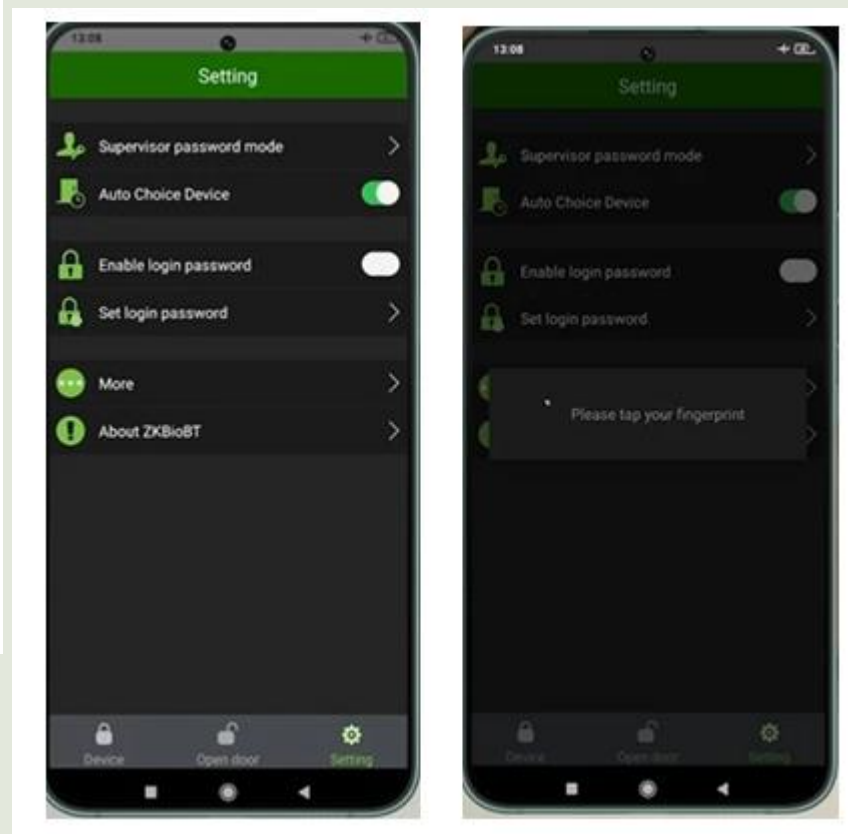
Ідентифікація за відбитком пальця



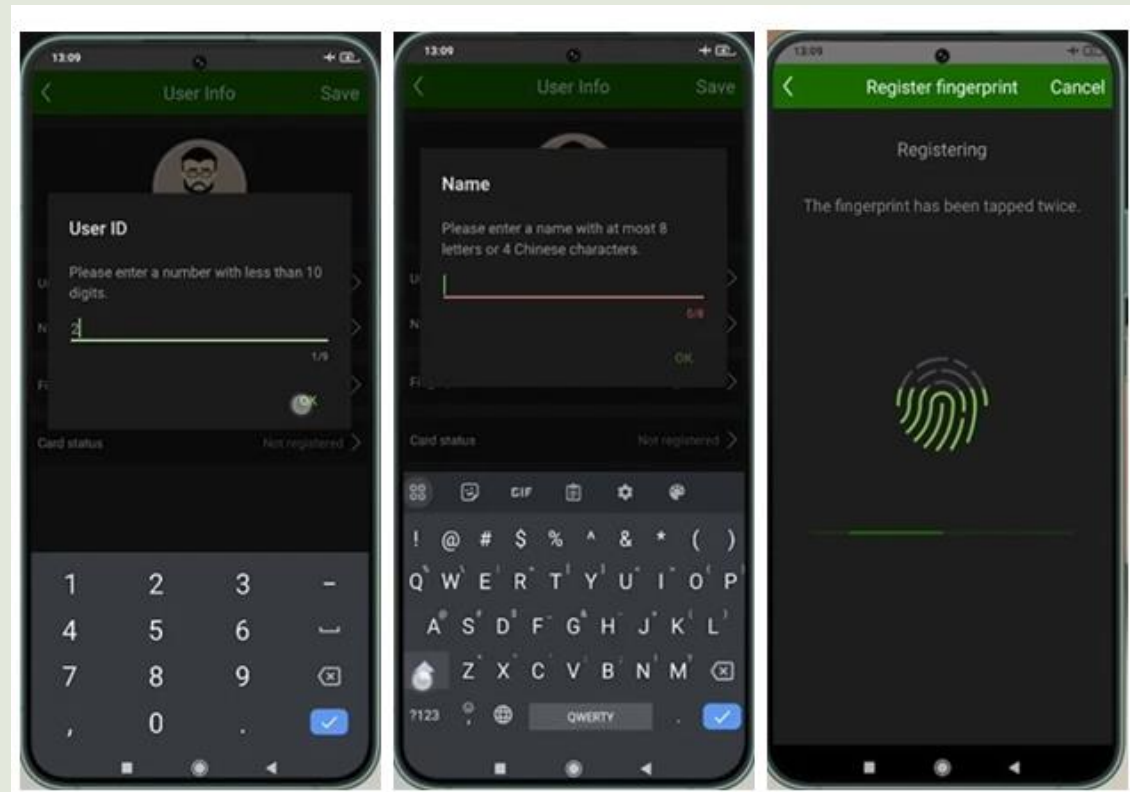
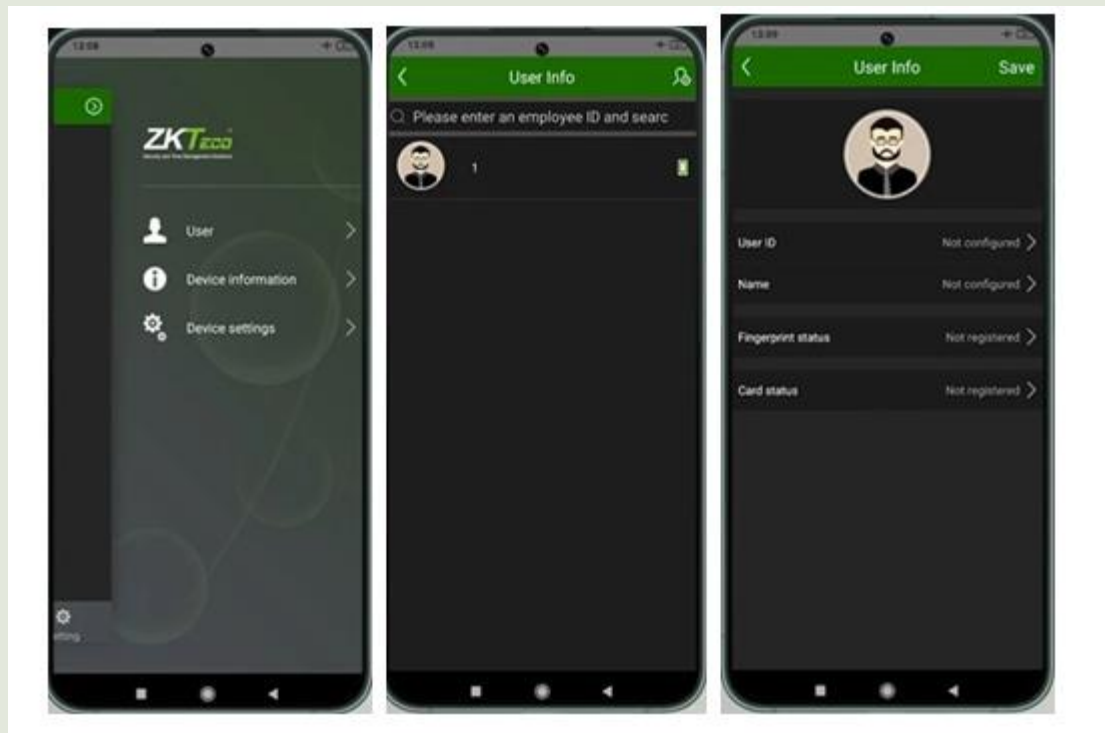
біометричний
термінал з Bluetooth
ZKTeco MA300-
BT/ID



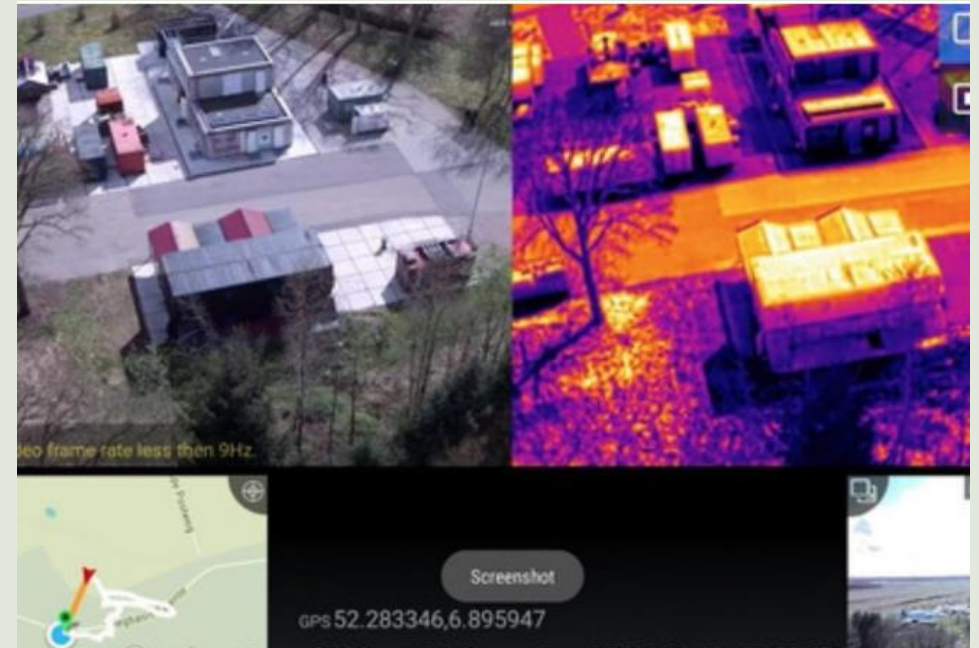
застосунок ZKBioBT



Ідентифікація за відбитком пальця



Використання дронів для охорони периметра критично важливого об'єкта



Квадрокоптер дрон DJI Matrice 350 RTK Enterprise + DJI Zenmuse H20T

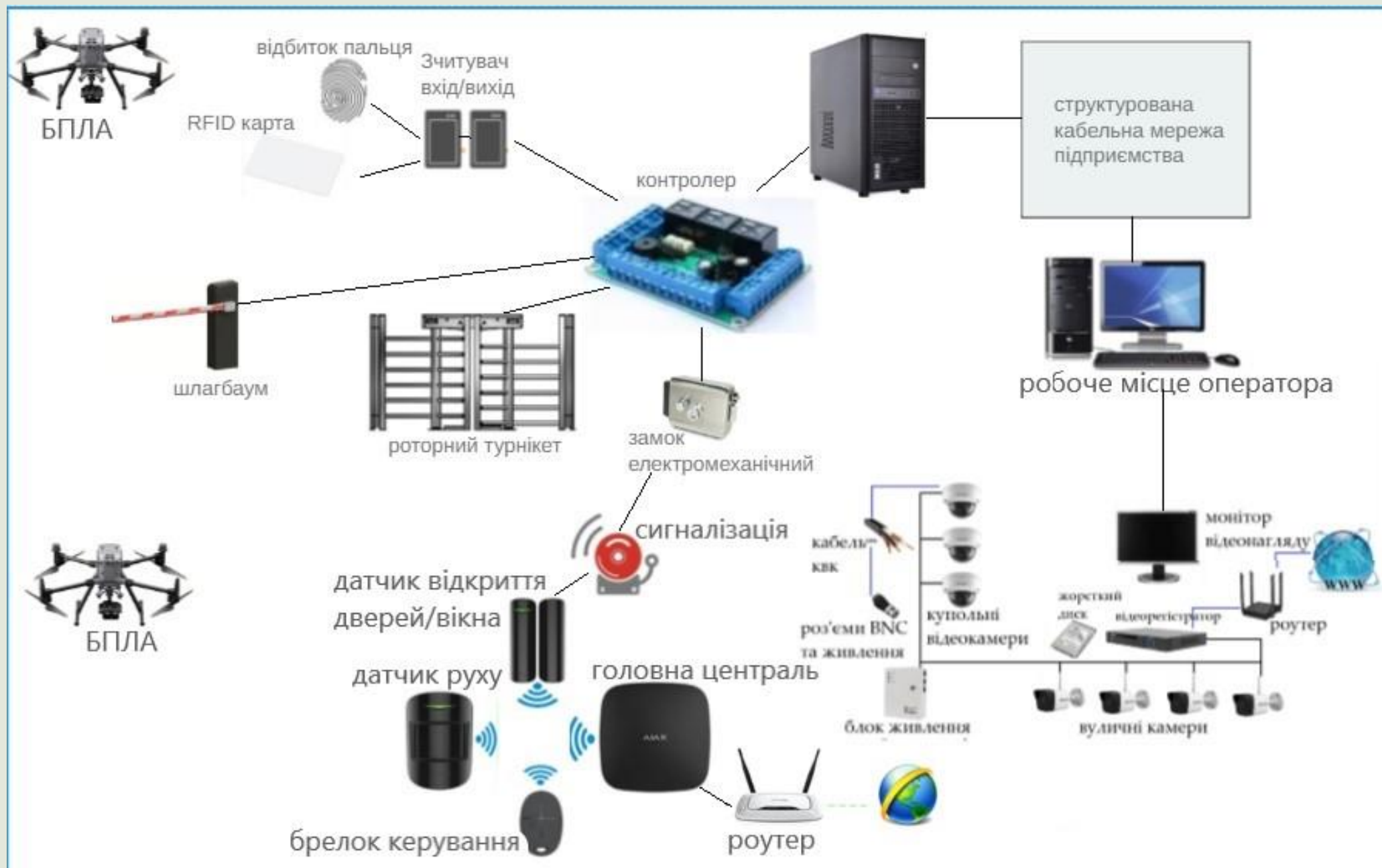
Застосування фреймворку Mitre ATT&CK. Процес моделювання векторів атак на компанію.

layer X +

selection controls layer controls technique controls

Розвідка 10 techniques	Розробка ресурсів 7 techniques	Початковий доступ 9 techniques	Виконання 13 techniques	Закріплення 19 techniques	Підвищення привілеїв 13 techniques	Ухилення від захисту 42 techniques	Доступ до облікових даних 17 techniques	Виявлення 30 techniques
<ul style="list-style-type: none"> Сканування IP-блоків Активне сканування (1/3) Vulnerability Scanning Wordlist Scanning Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/3) Search Closed Sources (0/2) Search Open Technical Databases (0/5) Search Open Websites/Domains (0/3) Search Victim-Owned Websites 	<ul style="list-style-type: none"> Acquire Infrastructure (0/7) Compromise Accounts (0/3) Compromise Infrastructure (0/7) Develop Capabilities (0/4) Establish Accounts (0/3) Сертифікати підпису коду Digital Certificates Exploits Шкідливе ПЗ Tool Vulnerabilities Obtain Capabilities (1/6) Stage Capabilities (0/6) 	<ul style="list-style-type: none"> Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Цілеспрямований фішинг з вкладенням Code Signing Certificates (T1588.003) Shimming Link Shimming via Service Replication Through Removable Media Supply Chain Compromise (0/3) Trusted Relationship Valid Accounts (0/4) 	<ul style="list-style-type: none"> Command and Scripting Interpreter (0/8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (0/3) Native API Scheduled Task/Job (0/5) Serverless Execution Shared Modules Software Deployment Tools System Services (0/2) User Execution (1/3) Windows Management Instrumentation 	<ul style="list-style-type: none"> Account Manipulation (0/5) BITS Jobs Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (0/4) Event Triggered Execution (0/16) External Remote Services Hijack Execution Flow (0/12) Malicious Image Malicious Link Модифікація процесу аутентифікації Implant Internal Image 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Create or Modify System Process (0/4) Domain Policy Modification (0/2) Escape to Host Event Triggered Execution (0/16) Exploitation for Privilege Escalation Hijack Execution Flow (0/12) Process Injection (0/12) Scheduled Task/Job (0/5) Valid Accounts (0/4) 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/10) Hijack Execution Flow (0/12) Impair Defenses (0/9) Indicator Removal (0/9) 	<ul style="list-style-type: none"> Adversary-in-the-Middle (0/3) Brute Force (0/4) Credentials from Password Stores (0/5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (0/2) Input Capture (0/4) Модифікація процесу аутентифікації Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (0/8) 	<ul style="list-style-type: none"> Account Discovery (0/4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Discovery Network Share Discovery Network Sniffing

Технологія інтелектуального захисту критично важливих об'єктів



Висновки

- Проведено класифікацію критично важливих об'єктів (КВО)
- Визначені потенційні впливи на КВО.
- Розроблена схема архітектури системи інтелектуального захисту КВО.
- Представлена архітектура системи штучного інтелекту для захисту КВО.
- Описаний алгоритм K-means та Random Forest для класифікації загроз.
- Запропоновано застосування ІОТ в системах інтелектуального захисту КВО.
- Розроблені моделі атак та визначені методи моніторингу загроз.
- Розроблений алгоритм реагування на інциденти загроз на критичну інфраструктуру.
- Здійснено вибір технічних засобів (система відеоспостереження, система керування доступом, сигналізація та оповіщення, протипожежна система), фізичних засобів захисту КВО – застосування БПЛА для охорони периметру об'єкта,
- Вибір фреймворків та механізмів для захисту КВО (MITRE ATT&CK) та розроблена сама технологія інтелектуального захисту КВО.

Дякую за увагу!